=WO 92/02103

⑲日本国特許庁(JP)　　⑪特許出願公表

⑫公表特許公報(A)　　平5－508274

⑬公表　平成5年(1993)11月18日

⑤Int. Cl.[5]		識別記号		庁内整理番号
H 04 B	7/26	109	S	7304－5K
H 04 M	1/00		N	7117－5K
H 04 Q	7/04		D	7304－5K

審査請求　有
予備審査請求　有

部門(区分)　7(3)

(全13頁)

⑤④発明の名称　電気通信システムにおける加入者の真正証明及び保護のための方法

㉑特　願　平3－512685
㉒㉖出　願　平3(1991)7月15日
㉕翻訳文提出日　平5(1993)1月8日
㉖国際出願　PCT/US91/04970
㉗国際公開番号　WO92/02103
㉘国際公開日　平4(1992)2月6日

優先権主張　㉜1990年7月16日㉝米国(US)㉞554,951

㉒発明者　フランダース・メアリー　ベス　アメリカ合衆国イリノイ州　60191、ウツドデイル、イロクオイス・トレイル　108
㉒発明者　フインケルスタイン・ルイス　デイ　アメリカ合衆国イリノイ州　60090、フイーリング、ウエスト・オツトワ・コート　1698
㉑出願人　モトローラ・インコーポレーテツド　アメリカ合衆国イリノイ州　60196、シヤンバーグ、イースト・アルゴンクイン・ロード　1303
㉔代理人　弁理士　池内　義明
㉛指定国　CA,JP

最終頁に続く

請求の範囲

1．暗号化プロセスを使用する電気通信システムにおける、加入者保護方法であって、

(a)加入者ユニットに関連する擬似ランダム数値の記録を維持する段階、

(b)前記記録を目標無線通信ユニットに通信する段階、そして

(c)前記加入者ユニットと前記目標無線通信ユニットとの間において前記記録を暗号化変数として使用し他の暗号化プロセスを利用する段階、

を具備する暗号化プロセスを使用する電気通信システムにおける、加入者保護方法。

2．前記擬似ランダム数値の記録は前記加入者ユニットに関するチャネルハンドオフの数の記録からなる、請求の範囲第1項に記載の方法。

3．無線電話通信システムにおける加入者ユニットと中央通信ユニットとの間での真正証明および保護方法であって、

(a)前記加入者ユニットに第1のIDおよび前記中央通信ユニット以外の目標通信ユニットを独自的に識別するターミナルエンドポイント識別子を提供する段階、

(b)前記第1のIDを前記中央通信ユニットから受信したランダム数の関数として変更することにより前記加入者ユニットにおいて変更された第1のIDを発生する段階、

(c)前記加入者ユニットにおいて前記変更された第1のIDを前記ターミナルエンドポイント識別子の関数として変更する段階、そして

(d)無線通信リンクを介して前記変更された第1のIDを加入者ユニットから中央通信ユニットに送信する段階、

を具備する無線電話通信システムにおける加入者ユニットと中央通信ユニットとの間での真正証明および保護方法。

4．さらに、

(a)前記加入者ユニットには第2のIDが与えられ、かつ

(b)前記変更された第1のIDは前記加入者ユニットにおいて前記第1のIDを前記受信されたランダム数および前記第2のIDの関数として変更することにより発生される、

請求の範囲第3項に記載の方法。

5．無線電話通信システムにおける加入者ユニットと中央通信ユニットとの間での真正証明および保護方法であって、

(a)前記中央通信ユニットに第1のIDに関する情報を提供する段階、

(b)前記中央通信ユニットにおいて前記加入者ユ

ニットからサービスの要求を受信する段階であって、該サービスの要求は前記中央通信ユニット以外の目標通信ユニットを独自的に識別するターミナルエンドポイント識別子を含むもの、

（ｃ）前記サービスの要求を受信したことに応じて無線通信リンクを介してランダム数を前記中央通信ユニットから前記加入者ユニットに送信する段階、

（ｄ）前記中央通信ユニットにおいて変更された第１のＩＤを受信する段階であって、該変更された第１のＩＤは前記第１のＩＤ、送信されたランダム数および前記ターミナルエンドポイント識別子から得られるもの、そして

（ｅ）前記中央通信ユニットにおいて、前記受信され変更された第１のＩＤ、前記受信されたターミナルエンドポイント識別子、前記送信されたランダム数および前記第１のＩＤに関する情報によって、前記受信されたサービス要求が真正のものであるか否かを判定する段階、

を具備する無線電話通信システムにおける加入者ユニットと中央通信ユニットとの間での真正証明および保護方法。

６．さらに、

（ａ）前記中央通信ユニットには第２のＩＤが与えられ、そして

（ｂ）前記受信されたサービス要求が真正のものであるか否かを判定する段階は前記第２のＩＤの使用を含む、

請求の範囲第５項に記載の方法。

７．（ａ）前記中央通信ユニットは前記加入者ユニットに対するホーム通信ユニットであり、そして

（ｂ）前記第１のＩＤに関する情報は実質的に前記第１のＩＤに等しい、

請求の範囲第５項に記載の方法。

８．（ａ）前記中央通信ユニットは前記加入者ユニットに対する訪問された通信ユニットであり、

（ｂ）前記中央通信ユニットに第１のＩＤに関する情報を提供する段階は、

（ｉ）前記訪問された通信ユニットが前記第１のＩＤに関する情報を有するか否かを判定する段階、

（ｉｉ）もし前記訪問された通信ユニットが前記第１のＩＤに関する情報を持っておれば、前記第１のＩＤに関する情報を回収する段階、そして

（ｉｉｉ）前記加入者ユニットに対するホーム通信ユニットと通信し、引続き前記第１のＩＤに関する情報を回収し、そしてその後、もし訪問された通信ユニットが前記第１のＩＤに関する情報を持っていなければ、前記第１のＩＤに関する情報を前記訪問された通信ユニットに格納する段階、

を具備する、

請求の範囲第５項に記載の方法。

９．無線電話通信システムにおける加入者ユニットと中央通信ユニットとの間での真正証明および保護方法であって、

（ａ）前記加入者ユニットに第１のＩＤおよび前記中央通信ユニット以外の目標通信ユニットを独自的に識別するターミナルエンドポイント識別子を提供する段階、

（ｂ）前記中央通信ユニットに前記第１のＩＤに関する情報を与える段階、

（ｃ）無線通信リンクを介して前記加入者ユニットから前記中央ユニットにサービスの要求を送信する段階であって、該サービスの要求は前記ターミナルエンドポイント識別子を含むもの、

（ｄ）前記中央通信ユニットにおいて前記サービスの要求を受信する段階、

（ｅ）無線通信リンクを介して前記中央通信ユニットから前記加入者ユニットにランダム数を送信する段階、

（ｆ）前記ランダム数を前記加入者ユニットにおいて受信する段階、

（ｇ）前記加入者ユニットにおいて前記第１のＩＤを前記受信されたランダム数の関数として変更することにより変更された第１のＩＤを発生する段階、

（ｈ）前記加入者ユニットにおいて前記変更された第１のＩＤを前記ターミナルエンドポイント識別子の関数として変更する段階、

（ｉ）無線通信リンクを介して前記加入者ユニットから前記中央通信ユニットに前記変更された第１のＩＤを送信する段階、

（ｊ）前記中央通信ユニットにおいて前記変更された第１のＩＤを受信する段階、そして

（ｋ）前記中央通信ユニットにおいて、前記受信された変更された第１のＩＤ、前記受信されたターミナルエンドポイント識別子、前記送信されたランダム数および前記第１のＩＤに関する情報を使用することによって、前記受信されたサービスの要求が真正なものであるか否かを判定する段階、

を具備する無線電話通信システムにおける加入者ユニットと中央通信ユニットとの間での真正証明および保護方法。

１０．（ａ）前記加入者ユニットには第２のＩＤが与えられ、

（ｂ）前記中央通信ユニットには前記第２のＩＤが与えられ、

（ｃ）前記変更された第１のＩＤは前記加入者ユニットにおいて前記第１のＩＤを前記受信されたランダム数および前記第２のＩＤの関数として変更することにより発生され、そして

（ｄ）前記受信されたサービス要求が真正のものであるか否かを判定する段階はさらに前記第２のＩＤの使用を含む、

請求の範囲第９項に記載の方法。

明　細　書

電気通信システムにおける加入者の真正証明及び保証のための方法

技術分野

その発明は一般的には通信システムに関し、かつより特定的には無線周波（ＲＦ）セルラ電気通信システムに関する。

発明の背景

セルラ無線電話システムは通常（移動または携帯用ユニットのような）加入者ユニットを含み、該加入者ユニットはＲＦ送信を介して固定ネットワーク通信ユニットと通信する。典型的な固定通信ネットワークは少なくともベースステーション及び交換センタを含む。加入者ユニットがアクセスする交換センタは彼の「ホーム」交換センタでなくても良い。この場合、該加入者ユニットはローマー（放浪者：ｒｏａｍｅｒ）と称される。彼がアクセスした交換センタ（「訪問された」交換センタと称する）は彼の「ホーム」交換センタと公共交換電話ネットワーク（ＰＳＴＮ）を介して通信する。固定ネットワーク通信ユニットの１つの義務は要求元加入者ユニットがシステムの認証または真正証明（ａｕｔｈｅｎｔｉｃａｔｉｏｎ）要求に合致した後該加入者ユニットに通信システムの使用を許可することである。典型的なセルラ電話通信システムにおいては、各加入者ユニットには電話番号（移動識別番号：ｍｏｂｉｌｅ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｎｕｍｂｅｒ）（ＭＩＮ）及びいずれの固定ネットワーク通信ユニットに対しても加入者を独自的に識別する識別番号（またはシリアル番号）（ＳＮ）が割り当てられる。各加入者ユニットはそれを他の加入者ユニットから区別する独自の識別番号を持っている。固定ネットワーク通信ユニットはデータベースを介してこれらの識別番号にアクセスすることができる。これらの番号はしばしば加入者がシステムを使用した時間に対し加入者に課金するために固定ネットワーク通信ユニットによって使用される。ローム中の加入者ユニットの場合は、前記「訪問された」交換センタは該加入者の「ホーム」システムのデータベースと通信して該加入者を真正証明しかつ課金しなければならない。もしこの通信が加入者ユニットが生成する各々の呼に対して必要であれば、かなりの呼のセットアップ遅延が生じるであろう。加入者が他のユニットに電話をかける場合、彼は彼が電話しようとする電話番号を入力する。ダイアルされた電話番号は固定ネットワーク通信ユニットに送信されるべきデータとなる。データはまたユニットの位置のような第３の通信ユニットに関する他の情報を含むことができる。

正当な加入者の識別番号の検出はＲＦの盗聴によりまたは無線電話取入者によるＭＩＮ／ＳＮの組み合わせの意図的なあるいは不注意による登録によって行なわれ得る。いったん加入者の電話番号及び識別番号が得られると（盗まれると）、泥棒は他の加入者ユニットをその盗まれた識別番号によって再プログラムすることができ、２つまたはそれ以上の加入者ユニットが同じＭＩＮ／ＳＮの組み合わせを持つことになる。セルラ無線電話システムは正当な識別番号を持たない加入者へのアクセスを否定する真正証明手順を持っているが、マルチユーザ（ｍｕｌｔｉｐｌｅ　ｕｓｅｒｓ）を検出しあるいは加入者の識別番号を知らず取入者の影響を実効的に中和する能力を持たない。従って、正当なユーザが泥棒の使用及び彼自信の使用の双方に対して課金される。

幾つかの真正証明技術が知られている。ＥＩＡ－５５３セクション２．３は各加入者がＭＩＮ及び工場で設定されたＳＮを持つことを規定する。加入者がコンタクトしようと試みている電話番号は該加入者によって固定ネットワーク通信ユニットに送信されるデータである。真正証明はＭＩＮおよび対応するＳＮが前記固定ネットワーク通信ユニットのデータベースに検出されればこのシステムによって承認される。残念なことに、ＥＩＡ－５５３はＭＩＮまたはＳＮが固定ネットワーク通信ユニットに送信される前に暗号化されることを要求しておらず、従って任意のＭＩＮまたはＳＮの直接的なＲＦ検出を可能にしている。さらに、この技術は取入者（ｉｎｓｔａｌｌｅｒ）からＭＩＮ／ＳＮを取得する泥棒に対する保護を提供しない。

他の真正証明技術がｔｈｅ　Ｇｒｏｕｐｅ　Ｓｐｅｃｉａｌ　Ｍｏｂｉｌｅ（ＧＳＭ）によって発生されるヨーロッパセルラ通信システム仕告に記述されている。セクション０２．０９，０２．１７，０３．２０及び１２．０３を参照。この方法はさらに加入者が固定ネットワーク通信ユニットに対して一時的な移動加入者ＩＤ（ＴＭＳＩ）をオープンに送信することを要求し、該固定ネットワーク通信ユニットは該加入者に対してランダム数を発生しかつ送信する。この暗号化技術は加入者ユニットがそのメモリから少なくとも３つの暗号化要素、所定の暗号キー、ＳＮ（個別加入者真正証明キー）及びＭＩＮ（国際移動加入者識別番号－ＩＭＳＩ）を自律的に回収することを要求する。加入者は次に前記暗号を使用してそのＳＮ及びＭＩＮを暗号化しＲＡＮＤを署名された応答（ｓｉｇｎｅｄ　ｒｅｓｐｏｎｓｅ：ＳＲＥＳ）に処理する。加入者ユニットはこの署名された応答を固定ネットワーク通信ユニットに転送し、該固定ネットワーク通信ユニットはそのＳＮ、ＭＩＮ及び暗号キーを加入者の一時的ＩＤ（ＴＭＳＩ）を使用してそのデータベースに対してチェックする。

固定ネットワーク通信ユニットはデータベースから取り出した情報を使用して同じランダム数に対してその応答を発生し、かつ加入者の署名された応答を固定ネットワーク

通信ユニットが発生した応答と比較する。もしこれらの応答が実質的に等価であれば、真正証明が承認される。ダイアルされた電話番号は真正証明が認可された後にのみ送信することが許容される。このシステムは加入者が異なるセル領域に入る度ごとにＳＮを暗号化しかつ一時的なＴＭＳＩを再割り当てすることによって侵入者からＭＩＮ／ＳＮを取得する試みに対していくらかの保証を与えることができる。

１つの技術は加入者のシリアル番号を送信の前に暗号化するけれども、いずれのシステムもマルチユーザを検出しない。試みの検出はいったん彼等がアクセスを獲得すると保安システムを維持するために重要である。さらに、（暗号化のために要求される）ランダム数の送信は呼が生成される度ごとに加入者ユニットと固定ネットワーク通信ユニットとの間での余分の通信を必要とし、これは送信エラーの確率を増大しかつ固定ネットワーク通信ユニットの真正証明プロトコルルーチンに対し送信ステップを追加する。さらに、真正証明はシステムがデータの受け入れを許容する前に認証されなければならない。従って、データは真正証明手順のステップが完了した後に送信されなければならない。

保安セルラシステムはまた真正証明が承認された後に通話の保証を提供する。セルラシステムにおいて一般的であるように、加入者ユニットの他のチャネルへのハンドオフが種々の理由のため必要である。これらは通信リンクの品質を維持し、加入者ユニット間の同一チャネル妨害を最小化し、かつトラフィックの分布を管理することを含む。ハンドオフはチャネル間の通信の転送を含む。チャネル化はタイムスロット、周波数、（スペクトル拡散形式のシステムのように）符号、及びこれらの媒体分割の種々の組み合わせの形式をとる。ハンドオフはセル内ハンドオフ、セル間ハンドオフ及びクラスタ間ハンドオフを含む。セル内ハンドオフは同じセル内のチャネル（音声またはデータ）の間の転送であり、セル間ハンドオフは異なるセルにおけるチャネル間の転送であり、かつクラスタ間ハンドオフは異なるセル制御ユニットを親とするセルにおけるチャネル間の転送である。音声及び／またはデータ情報がそのような情報のオーソライズされていない検出を避けるために暗号化される保安セルラシステムにおいては、ハンドオフは暗号化の完全性を維持するために付加的な複雑さを導入する。

提案されているＴＤＭＡ米国デジタルセルラシステムのような、ベースサイト間の絶対的なフレーム同期が要求されないシステムにおいては、加入者ユニットはそれらがハンドオフされた後にそれらがフレーム内のどのスロットに同期しなければならないかを教えられるだけである。しかしながら、保安システムにおいては、加入者ユニットといずれかの発信ベースサイト送受信機の間の音声の暗号化は通常同意されたスタート点を必要としかつハンドオフの数にかかわりなく呼の長さにわたり継続しなければならない。ハンドオフにおいては、通話はすでに進行中であり、従って暗号化の同期を確立するために必要な長いギャップは避けなければならない。また、通話における任意の点でチャネルを監視している侵入者は何等かの暗号解析の努力を助ける十分な情報を得ることができるべきではない。

１つの解決方法は暗号化アルゴリズムを音声の各スロットに対して再使用される共通のマスクによって動作させることを含む。しかしながら、これは同じ暗号マスクが各タイムスロットに対して反復されそれによって侵入者が同じ暗号化プロセスを分析しかつその結果暗号解読の確率を増大させる機会を反復して持つことができるようにするため暗号化プロセスの安全性をひどく害する。ハンドオフにおいて、これには発信ベースサイト（現在サービスしているベースサイト）から目標ベースサイトにこのマスクを受け渡すことを含む。これは暗号化プロセスがハンドオフチャネルに同期した状態になることを許容する。また、音声コーダは通話における休止（無音期間）の間にその出力シーケンスを発生し続けるから、侵入者はこれらの休止の間に暗号化プロセスを判定する良い機会を持つ。

他の解決方法は各ハンドオフにおいて暗号化プロセスを再スタートすることを含む。しかしながら、これは各ハンドオフの後に正確な暗号の流れを反復することを必要とする。ハンドオフが発生する度ごとに暗号の流れを侵入者がデコードする確率は大幅に増大し、特にマイクロセルラシステムにおいては顕著である。暗号化の方法は暗号解読をより困難にするために高度の変化性を与えなければならない。真正証明プロセスの間のように、暗号化プロセスにおいて使用される任意の変数は放送電波によって通信されるべきではない。

他の解決方法は連続的な流れの暗号化プロセスを使用し、この場合該プロセスは同じ通話に対するすべてのハンドオフの間その連続性を維持しなければならない。例えば、正確なスタート点は加入者ユニット及び発信ベースサイトによって同意されなければならない。ハンドオフにおいては、暗号化プロセスの現在の内容並びに転送の正確な点が発信ベースサイト及び目標ベースサイトによって同意される。この方法は容易には非同期システムに役立つものではなく、それは目標サイトは暗号化プロセスの現在の段階を知ることができないからである。また、ベースサイト間のメッセージの長さが増加するが、それは加入者ユニットによって開始される暗号化アルゴリズムの履歴を規定し目標サイトが暗号化プロセスの現在の状態を発生できるようにするため多数のメモリ要素が必要になり得るためである。

不正なユーザを検出しかつ効率的にオーソライズされていない検出から識別番号を保護するセルラ通信システムのための実質的に増強された真正証明技術の必要性が存在する。この技術は、「訪問された」システムが加入者ユニッ

トの合法性を判定できるようにしながら放浪者（ｒｏｍｅｒｓ）が「訪問された」システムを効率的にかつタイムリーな形式でアクセスできるようにすべきである。この真正証明方法はアクセスが不注意によって承認された場合に非合法なユーザのシステムを利用する能力を制限すべきである。さらに、暗号化から生ずる適切なレベルの保安性は真正証明プロセスの間における付加的な送信プロセスを要求すべきではなくあるいは高いエラーレベルを注入すべきではない。また、チャネル間のハンドオフの間における暗号化の完全性を提供し、侵入者が実質的に前記暗号化プロセスをデコードすることを防止する同期チャネルまたは非同期チャネルシステムにおいて使用するための暗号化プロセスの必要性が存在する。

発明の概要

これら及び他の必要性は実質的に以下に説明する電気通信システムにおける加入者の真正証明及び保証のための方法の提供によって満たされる。この方法は、加入者ユニットのような、第１の通信ユニットと、固定通信ユニットのような、第２の通信ユニットとの間で使用するための真正証明技術を示しており、この場合前記第１の通信ユニットは、第１の通信ユニット及び第２の通信ユニットの双方に知られた（シリアル番号のような）、ＩＤを、データを一つの暗号化キーとして、かつ（個人的識別番号－ＰＩＮのような）第２のＩＤを第２の暗号化キーとして、並びにネットワークが発行したランダム数（ＲＡＮＤ）を第３の暗号化キーとして使用し、変更する。加入者によって生成された電話呼の数のカウントまたは該加入者に対して発生したハンドオフの数のカウントのような、所定の通信の数の歴史的な非任意性の値は前記第１及び第２の通信ユニットの双方において維持される。この値（カウント）は歴史的なものであるが、それはそれがある通信ユニットに付与する過去の電話呼を表すからであり、かつこの値は非任意的なものであるが、それはこの処理の歴史（生成された呼の数）が同期外れの通信ユニットを識別するのに役立つからである。

第１の通信ユニットは（ＲＦ信号を介して）変更されたＩＤ及びカウントを第２の通信ユニットに送信する。第２の通信ユニットは第１の通信ユニットにより維持されるカウントを第２のユニットによって維持されるカウントと比較する。カウントの不一致は１つのユニットに対する異なる数の呼を示しそのカウントがシーケンス外である複数ユーザを示す。第２の通信ユニットは受信されたデータ及び知られた第２のＩＤを使用してその知られたシリアル番号によって同じ暗号化方法を遂行する。第２の通信ユニットは受信された変更シリアル番号及び固定ネットワーク通信ユニットにより発生されたシリアル番号を比較し該シリアル番号が有効であるか否かを判定する。本発明は通信ユニットの第１のＩＤのオーソライズされていない使用を実質的に低減するよう設計されている。該真正証明方法は第２のＩＤがＲＦによって送信されることを要求しない。

この発明は同じシリアル番号及び電話番号を使用する複数（マルチプル）加入者を検出するための方法を提供する。さらに、もしマルチユーザが送信された情報をコピーしかつ同じ情報をシステムにアクセスするために使用すれば、該マルチユーザは、彼自信の選択した電話番号ではなく、前記真正証明メッセージにある電話番号のみをかけることに限定される。この真正証明の発明はまた送信されたデータ及び第２のＩＤを、それらを暗号の一部として使用することにより、より効率的に使用できるようにして真正証明のエラーを低減し、前記暗号化手段は付加的なＲＡＮＤの流れが固定ネットワーク通信ユニットによって共通の暗号化ベースとして使用するために送信されることを必要とせず、かつそれによってこの付加的な送信を除去しかつ従ってエラーの確率を低減する。この真正証明装置はマルチ呼が「ホーム」システムから「訪問された」システムに送信されることを可能にすることによって効率的なローミングを可能にする。これらの真正証明変数は「訪問された」交換センタによって記憶されかつその後の呼に応じて使用することができる。この記憶は「訪問された」交換センタがすべてのその後の呼を「ホーム」システムへのリアルタイム通信なしにかつ関連する呼の設定の遅延なしに真正証明できるようにする。また、加入者のシークレットキー（ＰＩＮ）を「ホーム」交換センタに保持しかつ呼の個人的な情報を「訪問された」交換センタと共用しないことも重要である。

セルラサービスを盗む方法は、詐欺的に手に入れた移動装置からフラッシュを行い現存する呼を引継ぐことである。このフラッシュメッセージは固定ネットワークに正当なユーザがサードパーティの呼を生成していることを通知する。この問題に対する１つの可能な解決方法は固定ネットワークがそのトラフィックチャネルによって真正証明手順を開始することである。しかしながら、詐欺的に手に入れた移動装置は正当な移動装置が真正証明プロセスを完了することを可能にすることができる。この問題に対する他の解決方法は真正証明している移動装置に該移動装置がそれ自体に対して入手可能な情報のみを使用させることである。この解決方法に対する特定の実施例は前記フラッシュメッセージのダイアルされたデジットを真正証明アルゴリズムの出力と排他的ＯＲ（ＸＯＲ）演算を行いかつ次に、この応答を固定ネットワークに送信して正当な移動装置が現実にサードパーティの呼を生成していることを認証させることである。このような場合においては、詐欺的に入手した移動装置のみがそれが送信しているダイアルされたデジットを有するから、合法的な移動装置は前記フラッシュメッセージを正しく真正証明することができない。従って、固

定ネットワークは前記詐欺的に入手した移動装位からの呼を完了させない。

チャネルによって通信される暗号化情報に対して少なくとも１つの暗号化キーを利用する暗号プロセスを用いた保安セルラ通信システムにおいては、ハンドオフの間に暗号化の完全性を保つ方法は、ある加入者ユニットに関連する擬似ランダム文字の記録、例えば任意の数の発信無線通信ユニットとのある会話の間に該加入者ユニットが受けたハンドオフの数のようなもの、を維持する段階、侵入者による検出を防止するために磁気媒体などによって、前記記録を目標無線通信ユニットに通信する段階、および前記記録を暗号化変数として使用し前記加入者に対する他の暗号化プロセスを再スタートする段階を含む。

図面の簡単な説明

第１図は、典型的な加入者通信ユニットおよび固定ネットワーク通信ユニットのブロック図である。

第２図は、加入者通信ユニットによって使用される識別暗号化方法を示すフローチャートである。

第３図は、本発明に係わる固定ネットワーク通信ユニットによって使用される真正証明方法を示すフローチャートである。

第４図は、本発明に係わるハンドオフの間に暗号化の完全性を保持する方法を一般的に示すフローチャートである。

第５図は、本発明に係わる暗号化装置を一般的に示す説明図である。

第６図は、固定ネットワーク通信ユニットによって使用される別の真正証明方法を示すフローチャートである。

第７図は、第６図に示される真正証明方法によって除去されるセルラ通信サービスを盗む方法を示す説明図である。

動作の最良の形態

第１図は、加入者電話のような、加入者通信ユニット（１０）、およびセルラ電話ベースサイトおよび交換センタのような固定ネットワーク通信ユニット（２０）を一般的に示す。加入者通信ユニット（１０）はマイクロプロセシング段（１２）、不揮発性メモリユニット（１１）、無線周波（ＲＦ）段（１３）、からなり、これらすべては技術的によく理解されているものである。付加的な要素は、（電話番号ーデータを入力するための）電話機のキー入力パッドのようなデータ入力段（１４）、加入者呼シーケンスカウンタ（１５）、および暗号化シリアル番号と称される暗号化段からの出力（１６）を含む。

不揮発性メモリユニット（１１）内には（加入者ユニットのための）シリアル番号（１８）、ＰＩＮ（１９）、および（例えば、移動識別番号（ＭＩＮ）の性格をもつことができる）加入者電話番号（１７）が含まれる。ＰＩＮは加入者ユニットおよび固定ネットワークユニットにのみ知られた第２のＩＤである。例えば、それは加入者ユニットの導入者（ｉｎｓｔａｌｌｅｒ）に入手可能であるべきではなく、それは加入者ユニットの正当なユーザおよび固定ネットワーク通信ユニットのデータベースにとってのみ入手可能とすべきである。該加入者はＰＩＮをそれをアクティベイトするために一度だけ入力する必要がある。ＰＩＮは該加入者によって変更することができるが、その変更はまた固定ネットワークユニットにも知らされなければならない。これらの識別子は数字である必要はなく固定ネットワーク通信ユニットによって識別可能な任意の属性に対応することができる。別の実施例、例えば、セルラシステムにおいては、複数組のシリアル番号、ＰＩＮおよび電話番号を含むルックアップテーブルを記憶して含むことができ各組の識別子は特定のセルラ領域または固定ネットワーク通信ユニットに対応させることができる。

固定ネットワーク通信ユニット（２０）はマイクロプロセシング段（２２）、データベース（２３）、およびベースサイト無線周波数段（２１）へのリンクからなる交換センタを含み、これらの要素はすべて技術的によく知られている。付加的な要素としては固定ネットワークユニット呼シーケンスカウンタ（２４）および固定ネットワークユニット（２５）によって発生される暗号化シリアル番号が含まれる。さらに、交換センタは公共交換電話ネットワーク（ＰＳＴＮ）（６０）へのインタフェースを有する。ＰＳＴＮリンクは「訪問された」交換センタのためにローム中の加入者ユニットの真正証明および確認のために必要な「ホーム」交換センタへの通信のために使用できる。

前記データベースは加入者ユニットに関する情報、すなわちシリアル番号（１８）、ＰＩＮ（１９）、および加入者電話番号（１７）を含み、該情報はこれらのＩＤのコピーである。加入者通信ユニット（１０）のシリアル番号（１８）、ＰＩＮ（１９）および電話番号（１７）は固定ネットワーク通信ユニット（２０）に記憶されたシリアル番号（２８）、ＰＩＮ（２７）および電話番号（２６）に対応する。加入者通信ユニット（１０）と固定ネットワーク通信ユニット（２０）との間の通信はよく理解されたセルラシステム技術に従って２つのユニットの間でＲＦ送信を介して行なわれる。

加入者通信ユニット（１０）に真正証明が必要な場合、該加入者ユニットはそのシリアル番号（１８）を暗号化しかつその呼シーケンスカウンタ（１５）を増分する。第２図は、真正証明要求（２９）の間に固定ネットワーク通信ユニットに送信する前にそのシリアル番号を暗号化するために加入者通信ユニットによって使用される方法を示す。この方法は少なくとも２つの暗号化キーの使用を必要とする。加入者ユニットは呼ばれた電話番号（ＤＡＴＡ）（３０）をかつＰＩＮ（３１）をメモリから得、そしてこれら２つの要素の少なくとも一部をそのシリアル番号（３２）

を暗号化するために暗号化キーとして使用する。あるいは、加入者ユニットは呼ばれた電話番号（ＤＡＴＡ）、ネットワーク発行ランダム数（ＲＡＮＤ）（３０）、現在の加入者のシステム番号（歴史的データ）ならびにＰＩＮ（３１）を入手し、かつこれらの要素の少なくとも一部をそのシリアル番号（３２）を暗号化するための暗号化キーとして使用する。もしＰＩＮおよび呼ばれた電話番号がビットから構成されておれば、使用されるべきこれらのキーの前記一部はそれらのビットの内容および各キーのビット長である。例えば、暗号化シリアル番号は前記ＰＩＮまたはデータの内容に応じて、暗号化されないシリアル番号、または変更されない最初のＩＤ、とは異なるビット長を持つことができる。暗号化されたＳＮのビット長を変えることも加入者ユニットおよび固定ネットワークユニットの双方に知られた日時のような他の事象の関数としてもよい。

暗号化キーを統合するためのアルゴリズムはシステムの要求に応じて種々のレベルの保安性に適応するために変更することができる。真正証明応答メッセージの送信に先立つ最終ステップは電話番号（ｄａｔａ）を使用して暗号化されたメッセージを論理的に変換することである。この変換（ｔｒａｎｓｆｏｒｍａｔｉｏｎ）は「訪問された」交換センタがそれが前に加入者の「ホーム」交換センタから受信した記憶された真正証明変数を使用できることを保証する上で重要である。該「ホーム」システムによって発行された真正証明変数は前記電話番号（ｄａｔａ）について前記加入者が使用するという仮定を行なわない。従って、「訪問された」システムは該ＡＲＭをそれが「ホーム」システムから受信した真正証明変数および受信した電話番号（ｄａｔａ）に基づき計算することができる。この加入者の識別子の暗号化方法はデータが送信される前に真正証明が固定ネットワーク通信ユニットによって確認されることを必要としない。ＰＩＮをデータと組合わせることはＲＦ盗聴および加入者によるオーソライズされていない盗聴によるオーソライズされていない検出を実質的に除去するのに十分な程度にシリアル番号を復号コードに暗号化する能力を与える。

変更または修飾されたシリアル番号（暗号化されたＳＮ）は真正証明要求メッセージ（ＡＲＭ）（３５）の構成要素となり、これはＲＦ（３６）を介して固定ネットワーク通信ユニットに送信される。一旦暗号化が完了すると、割当てられた電話番号がメモリから得られる（３３）。この番号は真正証明手順の一部として暗号化されていない。この識別子はＡＲＭ（３５）の１つの構成要素であって固定ネットワークユニットに真正証明要求が有効な加入者ユニットから来ていることを通知する。

次に呼シーケンスカウントが得られ（３４）かつまたはＡＲＭにおいて使用される（３５）。該呼シーケンスカウントは真正証明手順が開始された時あるいは呼が完了した時のような所定の事象が発生するたびごとに更新される（加分または減分される）。該カウントは加入者ユニットおよび固定ネットワークユニットによってリングカウンタのようなロールオーバー形のカウンタを使用して維持することができる。このカウントは固定ネットワーク通信ユニットによって各加入者によって生成される呼の数をカウントするための手段として使用される。呼シーケンスカウントと組合わせて、あるいは呼シーケンスカウントの代わりに使用されるべき他の適切なカウントは該加入者ユニットに関連するハンドオフの数である。各加入者によって生成される呼の数の記録は加入者ユニットおよび固定ネットワーク通信ユニットの双方によって維持されるから、同じシリアル番号を使用するよう試みている他の加入者はそれが正当な加入者と全く同じ数の呼を生成していないから検出される。呼シーケンスカウント情報は真正証明要求メッセージの１つの成分として固定ネットワークユニットに通信される。ＡＲＭは任意の受入れ可能なフォーマットまたは任意の段数で通信できる。典型的なＡＲＭ（３５）の構成要素はデータ、暗号化シリアル番号、呼シーケンスカウント、および割当てられた電話番号を含む。別の実施例ではＳＮを変更するために使用される同じ暗号化方法を使用して呼シーケンスカウントを変更することを含む。これはさらに保証を強化するが、それは該カウントはまた前記ＰＩＮおよびデータを使用して変換されるからであり、各加入者は同じカウント（生成された呼の数）に対し異なる値を発生する。

固定ネットワーク通信ユニットは送信されたＡＲＭを受信しかつこの情報を加入者ユニットに対して真正証明が承認されるべきか否かを判定するために使用する。第３図は、固定ネットワークユニットによって行なわれる真正証明または認証方法を示す。ＡＲＭは固定ネットワークユニットでベースＲＦユニット（２１）によって受信される（３７）。固定ネットワークユニットはそのデータベースを介して有効加入者ユニットの割当てられた電話番号、シリアル番号およびＰＩＮにアクセスする。固定ネットワークユニットはその同じ割当てられた電話番号を固定ネットワークユニットのデータベースから得る（３８）ことによりＡＲＭで受信された割当て電話番号が有効であるか否かを判定する（３９）。加入者ユニットから受信された電話番号とデータベースにおいて検出された有効番号との間の比較が行なわれる（３９）。もし割当てられた電話番号が固定ネットワークユニットによって認識されなければ、真正証明は否定される（あるいは何らかの他の行動が取られる）（４０）。

もし割当てられた電話番号が有効であると判定されれば（それがデータベースにおいて検出されれば）、固定ネットワークユニットは次にそのデータベースからその特定の割当てられ電話番号に対応するシリアル番号およびＰＩＮ

を取出す。次に、固定ネットワークユニットはデータベースからのＰＩＮおよびＡＲＭにおいて受信されたデータを、加入者ユニットにおいて使用されるものと同じである、その暗号化方法（４４）の要素としての暗号化キーとして使用し、かつそれ自体の暗号化シリアル番号を発生する。固定ネットワークユニットはこの暗号化したシリアル番号を加入者ユニットによって暗号化されたシリアル番号と比較する（４６）。もしそれらが実質的に同じでなければ、システムはアクセスを否定するかあるいは何らかの他の所定の行動を行なう（４７）。もしそれらが受入れ可能な許容差内にあれば、受信された呼シーケンスカウントが得られ（４８）固定ネットワーク通信ユニットによって維持される呼カウント（４９）と比較される（５０）。もし該カウントが実質的に等しければ、真正証明は確証され（５２）これは第１の所定の過程の行動である。この時点で、加入者はダイアルされた番号に関連する第３の通信ユニットと通信することが許容され得る。この第３のユニットは、より一般的に、要求された（被要求）通信資源と称することができる。もし該カウントが受入れ可能な許容差内になければ、真正証明は否定されあるいは当局（ａｕｔｈｏｒｉｔｉｅｓ）にマルチユーザがシステムにアクセスしようとしていることを通知することができる（５１）。

固定ネットワークユニットの呼カウンタは真正証明が加入者に承認された回数を維持する。各加入者はそれ自身の呼カウンタを有する。加入者と固定ネットワーク通信ユニットとの間の連続的な呼カウント維持を持つことは他の加入者が何らかの他の加入者の識別番号を使用することを防止するが、それはその試みは正当な加入者が生成したのと同じ数の呼を生成しないからである。この不一致はネットワークユニットによって該ネットワークユニットが２つのカウントを比較した時にフラグ付けられる。

正当でないユーザに対する保証はさらに本暗号化方法が暗号化されたダイアル電話番号およびＰＩＮ（これは送信されない）を使用することによりさらに増強される。正当でないユーザが加入者のＰＩＮおよびシリアル番号を暗号化する正確なアルゴリズムを知らないため、試みは単に加入者の真正証明メッセージコピーしかつこのメッセージを反返すのみに限定される。加入者が異なる電話番号をダイアルするたびごとに、異なる真正証明要求メッセージが発生されるが、それは各加入者が異なるＰＩＮを持ち、各加入者が同じ電話番号に対し異なる真正証明要求メッセージを発生するからである。

試みは呼シーケンスカウントを検出し（それがＡＲＭにおいて暗号化されていないから）かつそれを更新することができるが、正しいカウントはその試みに彼が収取りした暗号化されたダイアル電話番号に対し真正証明を得ることができるようにするのみである。従って、不当なユーザはその暗号化された電話番号がＡＲＭからコピーされたものと整合する加入者にのみ通信することができる。

呼シーケンスカウントを備えた別の実施例は各加入者が１つより多くの呼カウンタを維持することを可能にし、この場合各固定ネットワーク通信ユニットに対する別個の呼カウンタが必要とされる。この実施例は加入者に複数の固定ネットワーク通信ユニットを使用できるようにするセルラ通信システムにおいて使用できる。第３図のフローチャートに対する他の実施例は呼シーケンスカウントを比較する段階（５０）が暗号化されたシリアル番号の比較を含むステップ（４６）の前に行なわれることを必要とする。

第７図においては、セルラサービスを盗む方法が示されている。特に、正当でないユーザ（７０４）は正当なユーザ（７０２）が有効な呼を生成するまで待機する。不当なユーザは次に正当なユーザ（７０２）とベースサイト（７００）との間のトラフィックチャネルをサードパーティのフラッシュ呼によって打勝つようにする（ｏｖｅｒｐｏｗｅｒｓ）。不当なユーザ（７０４）はベースサイト（７００）が正当なユーザ（７０２）に真正証明要求メッセージを送信する間に該トラフィックチャネルをドロップオフする。正当なユーザ（７０２）は該真正証明要求に対し正しく応答する。従って、ベースサイトは前記サードパーティ呼を接続する。一方、不当なユーザ（７０４）は前記トラフィックチャネルに打込ちかつ制御を得る。正当なユーザ（７０２）とベースサイト（７００）との間の元の呼は失われかつ正当なユーザ（７０２）は該トラフィックチャネルからドロップする。その結果、不当なユーザ（７０４）は呼ばれた前記サードパーティとの呼を維持しかつ該呼に対する該求Ｏは正当なユーザ（７０２）に送られる。

第６図においては、この形式のセルラサービスの窃盗を除去する方法が示されている。この除去は移動ユニットからの真正証明応答メッセージが、応答メッセージの少なくとも一部とダイアルされたデジットとの排他的ＯＲを含むことを要求することによって達成される。正当な移動ユニットは正当でない移動ユニットのダイアルしたデジットを知らないから、正当な移動ユニットは正しく真正証明せずかつ不当な移動ユニットのサードパーティ呼は進行しない。

次に第２図および第６図を参照すると、特に第６図はローム中の移動ユニットの真正証明をサポートする固定ネットワーク通信ユニットによって使用される別の真正証明方法を示す。この実施例においては、真正証明要求メッセージ（ＡＲＭ）がベースユニットのＲＦ段（２１）を介して固定ネットワークユニット（２０）によって加入者通信ユニット（１０）から受信される。該ＡＲＭは移動識別番号（ＭＩＮ）、ダイアルされたデジット（ｄａｔａ）および呼シーケンスカウントを含むことが好ましい。受信されたＡＲＭから、固定ネットワークユニット（２０）は該受信されたＡＲＭがそのホームネットワーク（６０２）における移動装置から来たか否かを判定する。

もし受信されたＡＲＭがホーム移動ユニットからのものであれば、固定ネットワークユニット（２０）はそのデータベース（２３）における割当てられたＭＩＮ（好ましくは電話番号）が該ＡＲＭ（６０４）において受信されたＭＩＮと同じであるか否かを判定する。移動ユニット（１０）からの受信されたＭＩＮとデータベース（２３）に見られる有効なＭＩＮとの間で比較が行なわれる。もし受信されたＭＩＮが固定ネットワークユニット（２０）によって認識されなければ、サービスは否定される（あるいは、何らかの他の行動がとられる）（６０６）。そうでなければ、もし受信されたＭＩＮが有効であると判定されれば（それがデータベースに検出されれば）、固定ネットワークユニット（２０）はデータベース（２３）から個人識別番号（ＰＩＮ）を取出しかつこのＰＩＮから特定のランダム応答対（ＲＡＮＤ／ＲＥＳＰ）を発生する（６０８）。ＲＡＮＤは好ましくはランダム数でありかつＲＥＳＰは好ましくはＲＡＮＤおよび前記特定の加入者のＰＩＮの関数として発生される数である。別の実施例では、ＲＥＳＰはＭＩＮ、電子的シリアル番号、および／またはローリングキーのような付加的な要素の関数として発生できることが理解される。その後、真正証明方法はステップ（６２２）において継続する。

これに対し、もし受信されたＡＲＭがホーム移動装置からのものでなければ、固定ネットワーク（２０）はこの訪問移動ユニットに対するＲＡＮＤ／ＲＥＳＰ対に対しそのデータベース（２３）をチェックする（６１０）。もしデータベース（２３）がこの訪問移動ユニットに対するＲＡＮＤ／ＲＥＳＰ対を含んでおれば、固定ネットワーク（２０）はこの特定の真正証明プロセス（６１２）において使用するために特定のＲＡＮＤ／ＲＥＳＰを取出しかつステップ（６２２）において真正証明プロセスを継続する。これに対し、もし固定ネットワークユニットのデータベース（２３）がこの訪問移動ユニットに対するＲＡＮＤ／ＲＥＳＰ対を含んでいなければ、固定ネットワークユニット（２０）は好ましくはＰＳＴＮリンク（６０）を介して訪問移動ユニットのホームネットワークをアクセスする。ホームネットワークはそのデータベースにおける割当てられたＭＩＮ（好ましくは電話番号）がＡＲＭ（６１４）において受信されたＭＩＮと同じであるか否かを判定する。訪問移動ユニットからの受信されたＭＩＮとホームネットワークのデータベースにおいて検出された有効なＭＩＮとの間の比較が行なわれる。もし受信されたＭＩＮがホームネットワークによって認識されなければ、サービスが否定される（あるいは何らかの他の行動がとられる）（６１６）。これに対し、もし受信されたＭＩＮが有効であると判定されれば（それがデータベースにおいて検出されれば）、ホームネットワークはこの訪問移動ユニットに対するＲＡＮＤ／ＲＥＳＰ対を好ましくはＰＳＴＮリンク（６０）を介して訪問ネットワークユニット（２０）に提供する（６１８）。固定ネットワークユニット（２０）はこれらの受信されたＲＡＮＤ／ＲＥＳＰ対をデータベース（２３）に格納する（６２０）。引続き、固定ネットワーク（２０）はこの特定の真正証明プロセス（６１２）において使用するために特定のＲＡＮＤ／ＲＥＳＰ対を回収しかつステップ（６２２）において真正証明プロセスを継続する。

真正証明ステップ（６２２）においては、固定ネットワークユニット（２０）はこの真正証明プロセスに対する特定のＲＡＮＤに関連するＲＥＳＰおよびＡＲＭにおいて受信されたダイアルされたデジットの論理関数（好ましくは、ＸＯＲ関数または他の非破壊的論理関数）であるＲＥＳＰ$_D$を発生する。引続き、固定ネットワークユニット（２０）は特定のＲＡＮＤを移動ユニット（１０）に発行する（６２４）。移動ユニット（１０）はこの特定のＲＡＮＤからネットワークユニット（ホームまたは訪問されたネットワークユニット）によって使用されるものと同じ方法である特定の方法を使用してＲＥＳＰを発生する。次に、移動ユニット（１０）は移動装置が発生したＲＥＳＰおよびＡＲＭにおいて送信されたダイアルされたデジットの論理関数（好ましくは、ＸＯＲ関数または他の非破壊的論理関数）であるＲＥＳＰ$_D$を発生しかつ移動装置が発生したＲＥＳＰ$_D$を固定ネットワークユニットに提供する（６２６）。固定ネットワークユニット（２０）はこの受信したＲＥＳＰ$_D$をネットワークユニットが発生したＲＥＳＰ$_D$と比較する（６２８）。もしそれらが実質的に同じでなければ、サービスは否定される（あるいは、何らかの他の行動がとられる）（６３０）。

あるいは、もし２つのＲＥＳＰＤが実質的に同じであれば、ＡＲＭにおいて受信された呼シーケンスカウントが固定ネットワークユニット（１０）によって維持される呼シーケンスカウントと比較される（６３２）。もしこれらのカウントが受入れ可能な許容差内になければ、サービスが否定され、当局はマルチユーザがシステムにアクセスしようとしていることを通知され（６３４）および／または何らかの他の適正な行動がとられる。これに対し、もし前記カウントが実質的に等しければ、真正証明は確認されかつサービスが発行される（６３６）。この時点で、移動ユニット（１０）はＡＲＭにおいて受信されたダイアルされたデジットに関連する第３の通信ユニットと通信することが許容されかつ真正証明プロセスが完了する（６３８）。

第４図は、ブロック４００で始まり、ここで発信（ｓｏｕｒｃｅ）ベースサイトは現在音声が加入者ユニットと発信ステーションとの間で通信されているトラフィックチャネルを保安するために第１の暗号化プロセスを使用している。一旦ハンドオフが要求されると（４０５）、加入者ユニットおよび近隣のベースサイトがよく知られた呼迂択技術を使用して迅切な目標サイトを決定する上で使用される。

辺切なチャネルおよび目標サイトが識別された後、現在のハンドオフカウントおよびセッションキーが陸線ネットワークを介して目標サイトに通信される（４１０）。加入者ユニットは新しいハンドオフチャネルを与えられ該チャネルによって目標ユニットと通信する（４１５）。該加入者ユニットおよび目標サイトは次にそれらのハンドオフカウントレジスタを変更する（４２０）。

目標サイトはチャネルが割当てられた後短い期間の間フレームカウントをＲＦリンクを介して加入者ユニットに送信する（４２５）。目標ベースサイトは加入者ユニットが正しいフレームカウントを獲得すれば該送信を中止する。従って、ハンドオフカウントが加入者ユニットおよび発信ベースサイトによって維持され、各ハンドオフに対して更新され、かつ通常各呼に対して独自のものとなる。ハンドオフカウントおよびフレームカウントの組合わせは擬似シークレット暗号同期変数として働く。目標サイトは受信されたハンドオフカウントを新しい暗号化変数として用い暗号化プロセスを再スタートすることにより目標チャネルによって加入者ユニットと通信を続ける（４３０）。

当業者には明らかなように、目標ユニットおよび発信（ｓｏｕｒｃｅ）ユニットは同じキャリア周波数からのタイムスロットの間でのチャネルのハンドオフの場合あるいはコード分割多重システムにおけるものと同じタイムスロットにおける他のコードへの転送の場合と同じ通信ユニットとすることができる。

暗号化の完全性を保つためのこの方法は目標サイトがハンドオフが発生するたびごとに通信をそこから継続するタイムスロットに対する新しい暗号化変数と真実的に同じランダムな変数を使用する。この方法はまた暗号化プロセスが各ハンドオフの後に再びスタートすることを強制し、それによって異なるサイトまたはチャネルからの音声コーダの間での近接的な暗号化プロセスの同期を必要としない。そのような暗号化組織は加入者および種々のチャネルの間のような、加入者ユニットに関連するハンドオフの擬似ランダム変数を使用してオーソライズされていない聴取者からの辺切な保証を保証する。任意の与えられた通話中に発生するハンドオフの数のランダム性の程度はセルの大きさ、伝送媒体の特性、加入者ユニットおよびベースサイトの受信機の感度、システムオペレータによって設定されたハンドオフしきい値のような要因、および種々の他の要因に依存する。その結果、マイクロセルラシステムおよび建物内システムにおけるハンドオフのカウントは大きなセルを有する地方のシステムよりもかなり多く変化する。これらの擬似ランダム変数とは異なり、日時または絶対フレーム番号（同期ＴＤＭＡシステムの場合などの）のような予測可能な変数は辺切な暗号化変数を与すが、それはこれらが同じ程度のランダム性を提供しないからである。侵入者は容易に経過時間の量を予測することができるが、それは最後の呼またはハンドオフは絶対フレーム番号を、それがＲＦ媒体を介して一般に送信されるため、容易に決定できるからである。同期ＴＤＭＡシステムの場合は、目標サイトは交換機、発信サイト、または他の辺切な手段から辺切なフレームカウント同期を決定できる。

第５図は、ハンドオフの間の暗号化の完全性を保つ方法を実行するための典型的な初期化ベクトル（５００）およびキーフィールド（５０５）に対するビットマップを示す。暗号化キーフィールドはセッションキーフィールドと称されるが、それはそれが各セッションまたは呼に対し独自のものでありかつ呼ごとのベースで変化するからである。初期化ベクトル（５００）は擬似ランダム暗号化変数を含みかつ加入者ユニットおよびベースサイトの双方によって維持されそして各スロットにつき変化する。初期化ベクトル（５００）は３２ビットを含み、かつこれら３２ビットはセッション暗号キー（５０５）と組合わされて各スロットに対して必要な１５９ビットを生成する。前記３２ビットは３つのカウンタ、すなわち８ビットのハンドオフカウンタ、９ビットの音声スロットカウンタ、および１５ビットの音声スロットオーバフローカウンタ、の間で分割される。ハンドオフカウンタは前に述べたように更新される。スロットカウンタには目標ユニットのスロットカウントが与えられ、かつオーバフローカウンタは呼の初めにおよびその後の各ハンドオフにおいてゼロのカウントからスタートされる。ベースサイトは加入者ユニットと、ＲＦを介して、各スロットの間に前記スロットカウンタの９ビットを、所定の時間の間、ＶＳＥＬＰ符号化または他の辺切な音声符号化方法を使用して発生できる、加入者ユニットからの音声を目標サイトが正しく暗号解読するまで、あるいは所定の時間が経過するまで、その送信の初めに送信することにより加入者ユニットと同期を確立する。

初期化ベクトルと組合わされたセッションキーフィールドは暗号化アルゴリズム（５１０）において使用され出力マスク（５１５）を発生し、該出力マスク（５１５）は音声（５２０）またはデータと排他的ＯＲされる（５１８）。次に、この出力はさらに知られたエラー保護技術を使用してエラー符号化される。

セッションキーおよびハンドオフカウントは陸線ネットワークによってベースサイトの間で通信されＲＦ侵入者による検出を防止する。加入者はそれ自体ハンドオフカウントを維持し、かつ固定ネットワークもまたカウントを維持するから、この情報をＲＦチャネルによって送信する必要がなく、それによってハンドオフカウントを擬似シークレット暗号変数にしておくことができる。

上述の方法はベースサイト間で絶対的なフレーム同期組織を持たないシステムにおける音声暗号化のための同期を提供する。しかしながら、当業者に明らかなように、ハンドオフの間に暗号化の完全性を保つための上記方法は容易

に任意の適切な保安セルラシステムに適用できる。チャネルハンドオフのカウントは好ましい擬似ランダム事象であるが、他の適切な擬似ランダム事象もまた与えられた加入者ユニットによって生成される呼の数、あるいは加入者ユニットが受ける電力の変化の数を含めて使用できる。当業者に理解できるように、擬似ランダム事象の記録はそのような事象のカウント以外の事象の他の表現を含むことができる。カウントを維持することは事象を表現する1つの方法に過ぎない。

当業者に明らかなように、数多くの別の実施例を特許請求された発明の精神および範囲から離れることなく考案できる。

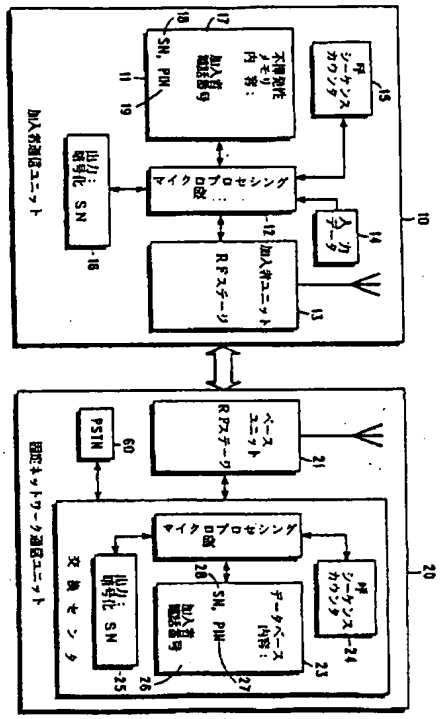

FIG.1

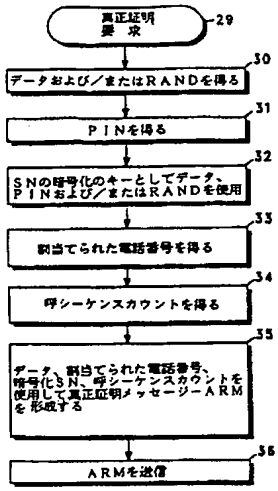

FIG.2

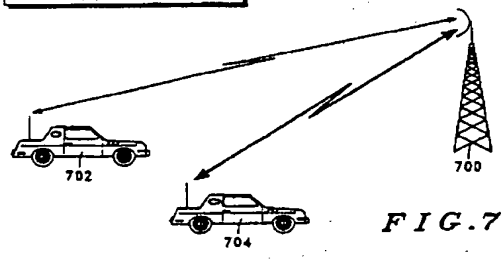

FIG.7

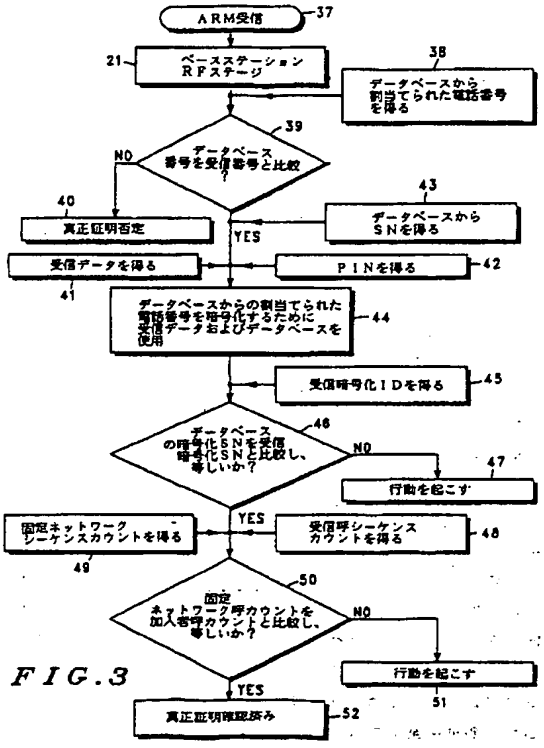

FIG.3

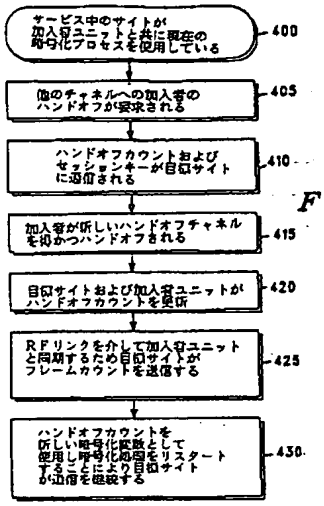

FIG.4

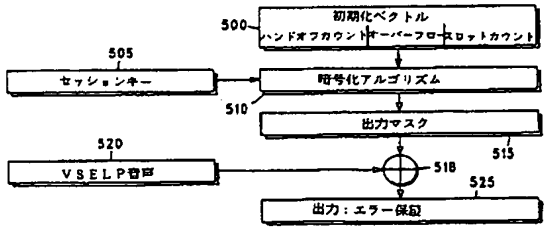

FIG.5

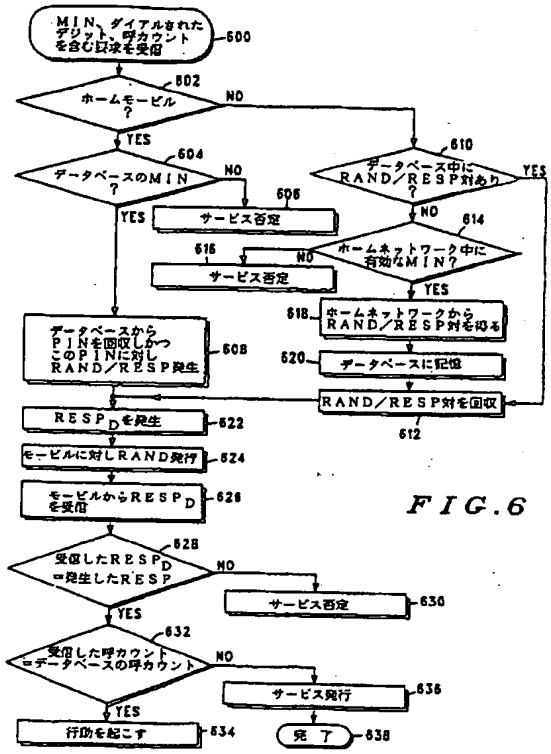

FIG.6

要　約　書

無線周波をベースとしたセルラ電気通信システムはしばしば加入者（１０）が所有者識別子（１９）またはシリアル番号（１８）を維持することを要求し、これは該加入者（１０）の真正を認証するために固定ネットワーク通信ユニット（２０）に送信される。暗号化および呼シーケンス方法が提供され、これは前記所有者ＩＤ（１８，１９）のオーソライズされていない検出を低減することができる。この方法はマルチ呼に対する真正証明変数が「ホーム」システム（２０）から「訪問された」システムに送信されかつ引続く呼によって使用するために「訪問された」システムによって記憶できるようにすることにより効率的なローミングを可能にする。さらに、前記真正証明移動ユニット（１０）にそれのみがそれ自身に利用可能な情報を使用させる方法が提供される。さらに、加入者ユニット（１０）と任意の発信無線通信ユニット（２０）との間で疑似ランダム事象（例えば、該加入者（１０）が与えられた通話中に受けるハンドオフの数）の記録を維持することによりハンドオフ中の近接した暗号化の完全性を可能にする方法を提供する。

国際調査報告

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all)
According to International Patent Classification (IPC) or to both National Classification and IPC
IPC (5): H04 Q 7/00
U.S.Cl. 340/825.340

II. FIELDS SEARCHED
Minimum Documentation Searched
Classification System: US
Classification Symbols: 340/825.340, 825.33, 825.69, 825.72, 825.3, 825.31; 379/59, 62,63
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched

III. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No.
Y	US,A, 4315101 (ATALLA) 09 February 1982 Note abstract; Fig. 1A, 3; col. 2, lines 25-40; col. 3, lines 45-70; as well as entire document.	1-10
Y	US,A 4816741 (HEBZO et al.) 21 March 1989 See col. 2, lines 60-70; col. 3, lines 56-70; col. 4, lines 20-31; and entire document	1-10
Y	US,A, 4023012 (AND et al.) 10 May 1977 See entire document	1-10

IV. CERTIFICATION
Date of the Actual Completion of the International Search: 21 August 1991
Date of Mailing of this International Search Report: 17 SEP 1991
International Searching Authority: ISA/US
Signature of Authorized Officer: Peter Wetzel

第1頁の続き

優先権主張 ㉜1990年12月7日㉝米国(US)㉛626,227

㉗発 明 者 ブール・ラリー シー アメリカ合衆国イリノイ州 60118、スリーピー・ハロー、プラム・コート 6